PhRMA

Alan Goldhammer, PhD
ASSOCIATE VICE PRESIDENT
US REGULATORY AFFAIRS

November 30, 1999

Dockets Managment Branch
(HFA-305)
Food and Drug Administration
5600 Fishers Lane
rm. 1061
Rockville, MD 20852

Re: Docket No. 99N-4166; Proposed Collection of Information Relating to 21 CFR Part 11; 64 Federal Register 53392

Dear Sir/Madam:

The Pharmaceutical Research and Manufacturers of America (PhRMA) represents the country's leading research-based pharmaceutical and biotechnology companies which are devoted to inventing medicines that allow patients to lead longer, happier, healthier and more productive lives. Investing $24 billion annually in discovering and developing new medicines, PhRMA companies are leading the way in the search for new cures.

Under the Paperwork Reduction Act, the Food and Drug Administration (FDA) has requested comment on the collection of information under certain provisions of the electronic records and signature rule (21 CFR Part 11). In spite of sincere efforts to implement FDA's 21 CFR Part 1 I regulation, PhRMA members have found it to be a major burden that is extremely difficult, if not impossible, to fully comply with. Representatives from our member companies have prepared the attached position paper that has been sent to Associate Commissioner Dennis Baker for consideration. It highlights the numerous issues that the pharmaceutical industry is facing as it moves to comply with the regulations. It is PhRMA's firm belief that both the FDA and industry need to work together to assure full and fair compliance with this regulation. As noted in the paper, there is no alternative to moving towards complete electronic record keeping.

We at PhRMA believe that the FDA's estimated paperwork burden is far too low. Companies will have several hundred computer systems falling under this regulation. All must be evaluated, documented, and, if necessary, a corrective action plan must be formulated, This may take anywhere from four to twenty hours, depending on what type of action plan needs to be developed. Thus, a company with 300 systems will face 3,200 - 4,000 hours just to assess the systems.

The estimates in this Federal Register notice also do not adequately assess the amount of time and money that must be spent to bring legacy systems (those in existence at the time the final rule went into effect) into compliance. Such systems were not grandfathered under the final rule. Thus, additional resources must be spent on

99N-4166

C4

validation activities, Standard Operating Procedures (SOPs), vender audits, and perhaps even replacement if the cost of bringing the system into compliance is deemed too high. It is likely that well over a hundred hours will be needed to bring a system into compliance. It is difficult to provide a quantitative estimate of this burden because it will vary significantly from company to company. However, this activity has the potential to add many more hours to the recordkeeping burden.

Finally, there is the ongoing burden associated with adding new computer systems and upgrading those already in service. System upgrades can take from two to ten hours to implement against the regulation. If one half of the 300 systems are upgraded, this would represent an expenditure of 1050 hours in compliance assessment.

Ignoring the hours needed to bring legacy systems into full compliance, PhRMA conservatively estimates the burden on the pharmaceutical industry to be in the neighborhood of 200,000 hours. FDA has calculated the total burden for all the FDA-regulated industries to be 270,000 hours. Thus, PhRMA believes that FDA's number is not realistic, both because of the cost to deal with legacy systems and because there will be costs to other industries in addition to the pharmaceutical industry.

Sincerely,

Alan Goldhammer

21 CFR Part 11
A Partnership Approach to Achieving Regulatory Compliance for Electronic Records and Signatures.

PhRMA, Position Paper Prepared by the
Information Management Working Group

15 November 1999

21 CFR Part 11
A Partnership Approach to Achieving Regulatory Compliance for Electronic Records and Signatures

Recommendations

As the pharmaceutical and biotechnology industries (hereafter referred to as the industry) move to manage their data in electronic form, the issue of ensuring regulatory compliance for electronic records, signatures and submissions becomes increasingly important. The FDA has taken a leadership role in this area leading to the March 1997 electronic records and electronic signatures regulation contained in 21 CFR Part 11 (hereafter referred to as the Regulation).

While the industry strongly supports the general principles embodied in the Regulation, the experience gained attempting to implement it has highlighted a number of practical difficulties. Given the joint commitment of FDA and industry to achieve a high level of GxP compliance, this paper proposes a partnership approach aimed at meeting the requirements of the FDA in a manner compatible with the capabilities of available technology. The proposal is based on a realistic assessment of the time and expense required to modify current systems or migrate to new ones, and addresses the problems posed by the long term archiving of electronic data.

Making the transition to electronic record keeping comes at a time when the industry is heavily involved in upgrading current systems to ensure that they are year 2000 compliant (Y2K). For most large pharmaceutical companies, Y2K has involved expenditures in excess of one hundred million dollars and posed a major challenge in terms of the number of systems covered and the resources required.

Upgrading systems to meet this new Regulation adds an additional element of risk and is a factor that needs to be considered in establishing the time needed. A period of 10 years may be necessary to implement the required changes in all affected systems.

In order to achieve a high level of sustainable compliance in the electronic environment, the industry proposes the following recommendations based on its current experience:

1. Requirements for systems should reflect current best practice procedures within the industry and take account of the capabilities provided by the major software packages used by the industry.

2. Where requirements for systems necessitate capabilities beyond those provided by the current generation of software systems, a realistic amount of time should be allowed for vendors to develop the required software and for the industry to implement it. The industry has a strong preference for the unmodified use of commercial products from market leaders.

3. Requirements for systems necessitating the introduction of new technologies, such as those associated with electronic signatures and a public key infrastructure, should take into account the risks associated with early adoption and the time for such technologies to mature and be incorporated into major software packages.

4. The point at which data becomes an electronic record should reflect its origin and intended purpose. For a manufacturing record this may be the initial point of data acquisition but for a clinical trial system it may be from the time the data are first committed to the official database, or for a clinical trial report it may be from its first official use.

5. The impact of the rapid obsolescence of technology should be considered in defining long term archival requirements for electronic data.

6. Realistic assessments of the costs and risks associated with required changes should be considered and balanced against a similar assessment of the expected reduction in risk to public health.

These recommendations will help to ensure that the industry can comply with the requirements of the Regulation taking account of current best practice, the capabilities of the current generation of information systems used in the industry, the risks associated with the adoption of new technology, and the time required for vendors to develop the required software and the industry to implement it. It will also help to ensure that the costs and risks associated with proposed changes are considered and commensurate with the expected reduction in risk to public health.

The industry and the regulatory agencies have a common goal in promoting best practice and improving public health. Adopting a partnership-based approach in this area of common interest should help to ensure that the industry has a better understanding of the requirements of the FDA and that regulations are based on current best practices within the industry and consider the costs and risk associated with proposed changes. By working together in this area, FDA and industry can ensure that the public benefits by having rapid access to new medicines with a high level of assurance of quality at reasonable cost.

The next sections of the document provide an overview of the reasoning behind the specific recommendations and are followed by appendixes providing specific comments on the guidelines and Regulation.

Rationale for the Proposed Recommendations

The reasoning behind these recommendations is summarized below.

I. Requirements of the Regulation should reflect current best practice procedures within the industry and take account of the capabilities provided by the major software packages used within the industry.

2 1 CFR Part 11 represents an extensive and careful study by the agency of the challenges posed by the move from paper-based to electronic records and the requirements of the Regulation for electronic records and signatures. The Regulation/Rule is seen by the industry as providing a desired future state with which they are keen to comply and indicates that the use of electronic records and signatures is voluntary and that industry is free to continue with the use of paper-based systems. However the FDA's goal of achieving paperless submissions by the year 2002 is incompatible with the option to continue using paper-based systems.

The major challenges faced by the industry in achieving compliance with the Regulation/Rule derive from two key sources. The first is that the ruling defines a desired future state but is not based on current best practices within the industry or the capabilities of the current generation of major software products that are in place. The second is that the industry already relies heavily on the use of electronic systems so that the option of reverting to a paper-based system is not viable. The consequence of this is that the industry has no option other than to do their best to comply with 2 1 CFR Part 11. Since the ruling is not based on current best practice within the industry, or the capabilities of the current generation of systems, it is not unexpected that most current systems do not fully meet the requirements for compliance

While the industry is committed to achieving compliance, the time required for vendors to provide the required software and for the industry to upgrade or replace the current generation of systems means that this will take a significant period of time (much longer than the 90 days stipulated in the Regulation). Hence, it is proposed that requirements should be based, where possible, on current best practice in the industry and take account of the costs and risks associated with major change.

The growing trend towards outsourcing and disintermediation within the industry also places a premium on the use of common software packages and standards, as data needs to be shared across multiple organizations. Hence, the following interim approach to achieving full compliance is proposed:

i. Identify those elements of the Regulation that can be achieved using commercial software packages currently used in the industry.

ii. Where the requirements can not be met directly using current software packages, explore alternative options to meet these requirements based on the available functionality.

iii, Where new functionality is required to meet the requirements, recognize the time taken by software vendors to respond and the risks and costs associated with upgrading or replacing major systems.

Where compliance can be achieved using the functionality available in the current generation of software packages used in the industry, or the requirement can be redefined to allow it to be achieved with current software, it should be possible to implement these changes relatively quickly. Given the potential need to reconfigure and retest current software, revalidate and document the changes and re-train users, a time period on the order of 12 months would seem realistic for each system or functionality. Where new functionality is required, the time is likely to be significantly longer, perhaps 10- 15 years, as described below.

The partnership of FDA and PhRMA is even more important in order to develop a strategy for vendors to be able to ensure that they have correctly interpreted the Regulation and have correctly built their software packages.

2. Where requirements for the Regulation necessitate capabilities beyond those provided by the current generation of software systems, then a realistic amount of time should be allowedfor vendors to develop the required software and for the industry to implement it. The industry has a strong preference for the unmodified use of commercial products from market leaders.

For several years now, the trend within the industry has been away from custom software development towards the use of commercial software packages. Despite its economic strength, the relatively small size of the industry (only a few hundred firms worldwide) means that its ability to influence software vendors is variable. Companies that specifically target the pharmaceutical industry, such as LIMS and clinical trial software vendors, or companies that generate a significant proportion of their revenue from the industry, such as SAP and Documentum, are normally willing to modify their software to make it compliant.

Even where vendors see a commercial advantage in being able to offer compliant software, the time taken to generate new releases is normally 12-24 months. Although the FDA often gives advance notice of proposed changes in requirements, most software vendors are unwilling to invest in modifications to their software until the requirements are final.

The time required by the industry to implement a major software release is, typically, 6-12 months depending on the size and complexity of the system and the number of automated links to other systems. Upgrades often involve modifying work processes, testing and validation, updating system and process documentation and additional training. Hence the total time to achieve compliance is often 18-36 months. Even this is conservative, as most companies are reluctant to implement the first version of a major new software release, preferring to wait for the second release so that the initial round of problems have been detected and resolved. The time required to upgrade a system depends on the size, complexity and the number of links to other systems. For a small, stand-alone, system it may be possible to replace it in 6- 12 months. However, for larger and more complex systems, this is likely to take at least l-2 years, thereby requiring many years to fix all affected systems.

There are also many vendors, such as Microsoft and IBM, for whom the pharmaceutical industry represents only a relatively minor portion of their overall revenue. These companies are typically reluctant to customize their software to the needs of a particular industry. This is especially true in the case of operating system software where the emphasis is normally on stability and backwards compatibility and it is unlikely that new functionality would be added to meet the particular needs of a single industry,

In this case, FDA needs to balance the risks of ensuring that compliance can be achieved with current products versus the risks arising from attempts to customize these products, either by the industry or a third party vendor, or the adoption of products from much less well established vendors. The industry perspective on the associated commercial risks is a strong preference for the unmodified use of commercial products from market leaders.

3. Requirements necessitating the introduction of new technologies, such as those associated with electronic signatures and a public key infrastructure, should recognize the risks associated with early adoption and the time taken for such technologies to mature and become incorporated into major software packages.

The introduction of new technologies, such as those required to provide authentication of electronic signatures, is a slow process. Typically, it takes 2-3 years for major new technologies, such as those associated with a Public Key Infrastructure (PIU) to support electronic signatures and authentication, to be incorporated into major software products. Early releases of these products are often unreliable and subject to rapid change as vendors work to remove defects and deliver the required functionality.

Hence, the industry is normally slow to adopt these technologies for use in mission critical and regulated systems, seeing them as representing a high level of business risk. Vendors tend to adopt a similar approach and it is often several years before new technologies are incorporated into major software packages.

Since one of the goals of electronic signatures is to ensure that they are non-repudiatable and legally enforceable, which adds an additional level of complexity, questions around the issuing and validation of keys, and whether this can be done by individual companies or will require trusted third parties, still need to be resolved. Ultimately, the validity of these new approaches needs to be tested in litigation and it is likely to be 3-5 years before they are widely used in major business systems.

4. The point at which data becomes an electronic record should reflect its origin and intendedpurpose. For a manufacturing record this may be the initial point of data acquisition but for a clinical trial report it may be from its first official use.

For key manufacturing systems, it is reasonable to define the electronic record as being created the first time that data is acquired and for it to be subject to an audit trail from that point forward. This may also be true for most transaction-based systems in which the initial transaction creates a record which is subsequently extended or modified. However, routine procedures such as double data entry, which is often outsourced, should not require an audit trail and the electronic record should be viewed as being created when this process is complete.

In the case of electronic documents, such as a clinical trial report, the data have normally already been generated and the purpose of the document is to provide context, analysis, evaluation and meaning. In practice, such documents are often created by one or more authors creating drafts, typically in the desktop environment, which may then be merged to form the initial version of the document. It is difficult to see these early component drafts as electronic records requiring formal audit trails and change control.

The starting point to introduce electronic signatures and an audit trail would appear to be the first official use of the document. This may be to obtain comments on a protocol or study report from a regulatory agency. Such an approach would simplify document creation, particularly while work is being carried out while traveling or off-site, without compromising its integrity.

Similar arguments would apply to the assembly of a regulatory submission. Since none of the component documents, each of which has its own associated audit trail, is modified and no new material is added, it is difficult to see the need for a formal audit trail for submission assembly. Once a submission has been assembled and submitted to a regulatory agency, it would then become an electronic record subject to an audit trail.

5. The impact of the rapid obsolescence of technology should be considered in defining long term archival requirements for electronic data.

This is a major challenge facing all systems where the data is stored in electronic form but needs to be retained for an extended period. The traditional approach is to print out data in paper form, or on microfilm or fiche, recognizing that it is not practical to preserve the electronic data over a prolonged period.

As part of the Regulation, the FDA has expressed the desire to retain access to the data in electronic form over the full retention period required for the associated electronic records, Given the rapid rate of obsolescence of technology, it is not clear how such long term, often 10-20 years, electronic access can be provided. Retaining the initial technology is not a viable option, as support from the vendors for the hardware and software becomes unavailable 2-5 years after the product has been superseded, and new hardware and software are not normally compatible.

Migrating the data to a new system is possible but this is an expensive option, given the level of re-validation required, and would need to take place on a 5-7 year basis. Hence, given the current state of technology, it is probably unrealistic to expect to preserve fully functional access to electronic data over an extended period. There are a number of data formats, such as Oracle and SAS data sets, and the Portable Document Format (PDF), from Adobe, that are likely to endure over the time scales required. Some of the emerging media formats, such as Digital Versatile Disk (DVD) may also have a reasonable life of 5-10 years. Hence, it will be necessary for the FDA and industry to work together to agree on a realistic approach, recognizing the risks, *costs* and limitations involved.

6. Realistic assessments of the costs and risks associated with required changes should be balanced against a similar assessment of the expected reduction in risk to public health.

21 CFR Part 11 gives the impression that the changes required to achieve compliance can be accomplished in 90 days at modest cost. As noted in the preamble to the Regulation, the rule is voluntary. As such, the FDA concluded that industry would incur no net cost as a result of the rule, assuming that “no firm (or regulated entity) will implement electronic record keeping unless the benefits to that firm are expected to exceed any costs (including capital and maintenance).” However, in reality, companies use electronic records not as a matter of choice but because it is an absolute necessity as a result of the large quantity of information required. The long-standing practice of printing critical information (including paper audit trails), validating and signing the printout and keeping the paper, or its PDF version, as the regulatory record has worked well. This is current practice and has been acceptable to agencies worldwide. Companies should be able to continue using approaches that were acceptable to the FDA prior to publishing the Regulation. The Regulation should apply only to changes in the process such as where true electronic signatures are used in place of the “print and sign paper” approach.

Although the Agency concluded that the Regulation will not have significant economic impact, PhRMA companies are estimating the financial impact to be significantly higher than the cost of resolving any Y2K problems, especially in light of the interpretation FDA officials have presented over the last two years. The work that has been done for the Y2K was to remedy one thing, changing a date. The changes necessary to be compliant with this Regulation are far more complex. In one case, it cost $600,000 to bring a chromatography system into compliance. There are hundreds of such systems that are bound by the Regulation. One large company has estimated that archiving a complex electronic system would cost them in excess of ten million dollars over the retention period. The cost to fully comply with the Regulation is expected to exceed $150 million for a large pharmaceutical company. In order to meet FDA’s interpretations, the pharmaceutical industry believes this burden is financially intolerable and not a value-added cost to the consumers, the patients.

Compliance with the Regulation requires upgrading or replacing most current systems and, potentially, the introduction of new, and relatively unproved, technologies. Experience in the industry shows that change programs on this scale carry a significant degree of risk and expense. Hence, the benefits expected from the Regulation need to be balanced against the risk and costs associated with its implementation. Few companies would attempt to complete changes on this scale in less than 10- 15 years. Attempting to accelerate this process would significantly increase the cost and level of risk. Although the cost would be much less for small biotech companies it could still be sufficient to put their survival at risk or make them vulnerable to takeover by larger companies . The Regulation should apply to new systems, not to the old systems that have been in place prior to the Regulation, or a jointly agreed set date, and the long term archival requirements should be eliminated or redefined.

Appendix A
Comments on 21 CFR Part 11 Guidelines

Summary

. . . The use of electronic records as well as their submission to FDA is voluntary...

Since most companies already make extensive use of computer systems, and therefore have a hybrid environment containing both electronic and paper records, it is not viable for them to revert back to a paper based system. Hence, in practice, they have no option other than to comply with 2 1 CFR Part 11. The industry is willing to do this but recognizes that it will require significant time and expense, given the large number of systems involved.

I. Effective Date/Grandfathering

9. . . . The agency believe that firms that have consulted with FDA before adopting new electronic record and electronic signature technologies (especially technologies that may impact on the ability of the agency to conduct its work effectively) will need to make few, if any, changes to systems used to maintain records required by the FDA.. .

The major issue is not around adopting new technologies. Most companies already have a large number of systems that now need to be made compliant. It is not possible to achieve this in the 90 days allowed by the Regulation and will, in fact, require significant time and expense. Hence, a time line of 18-36 months for each function or system, as recommended in this proposal, is more realistic and is consistent with the recorded comments in this section that it would require from 10 to 15 years for all systems.

IV Scope (11.1)

30. *. . . Persons should also be mindful of the need to keep appropriate computer systems that are capable of reading electronic records for as along as those records must be retained. In some instances this may mean retention of otherwise outdated and supplanted systems, especially where the old records cannot be converted to a form readable by the new systems. In most cases, however, FDA believes that where electronic records are accurately and completely transcribedfrom one system to another, it would not be necessary to maintain older systems. . . .*

Given the rapid obsolescence of technology it will be necessary to migrate data from one system to another on a 5-7 year basis. Since it is unlikely that the old and new systems will be identical, the cost of quality assuring and validating the data in the new system will be significant. It is also unlikely that the new system will display the data in the same way as the previous system.

There is also the question of how far these requirements will be carried. While it appears reasonable to want to be able to retrieve data for patients in clinical trials, it seems unlikely that the hardware and software used to generate the random numbers used in these trials would need to be retained.

A reasonable approach would be to archive data in agreed electronic formats such as Oracle and SAS data sets and PDF formatted documents. These are standards that are likely to endure and should provide reasonable assurance that the information can be accessed over the life of the electronic record.

V. Implementation (11.2)

36. ... The agency expects to work closely with industry to help ensure that the mechanics and logistics of accepting electronic submissions do not pose any undue burdens...

The industry is committed to working closely with the agency in this regard and the current proposal has been developed in this spirit of partnership.

VII. Electronic Records - Controls for Closed Systems (11.10)

57. . . . One comment expressed full support for the list of proposed controls, calling them generally appropriate and stated that the agency is correctly accommodating the fluid nature of various electronic record and electronic signature technologies. Another comment, however, suggested that controls should not be implemented at the time electronic records are first created but rather only after a document is accepted by a company.

The agency disagrees with this suggestion. To ignore such controls at a stage before official acceptance risks compromising the record. For example, if "pre-acceptance" records are signed by technical personnel, it is vital to ensure the integrity of their electronic signatures to prevent record alteration, The need for such integrity is no less important atpre-acceptance stages than at later stages when managers officially accept the records. The possibility exists that some might seek to disavow, or avoid FDA examination of, pertinent records by declaring they had not been formally "accepted". In addition, FDA routinely can and does inspect evolvingpaper documents (e.g. standard operating procedures and validation protocols) even though they have yet to receive a firm's final acceptance. ...

For transaction based electronic records that capture data and control information, it is reasonable to require *"procedures and controls designed to ensure the authenticity, integrity, and confidentiality of the electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."*

In the case of electronic documents, such as clinical trial reports, which provide an interpretation of data drawn from electronic records that are already subject to such controls, there is no clear need to re-impose these controls until the document is used for some official purpose.

Most authors prepare documents electronically in the desktop environment and go through many drafts. There may also be multiple authors so that the component drafts need to be merged to form the document. The cost and complexity of imposing the proposed controls at this early stage would be significant, since they are not supported by standard desktop software, and would limit the ability of staff to prepare drafts while traveling or when remote from a site.

Hence, a more reasonable approach would be to apply these controls at the point at which a document is first used outside the normal internal authoring, review and approval process. This could also be the point at which these documents become electronically "signed," matching the normal paper-based process. Given that some documents are circulated outside the internal authoring and review process, such as the review of a clinical trial protocol by the FDA or other regulatory agency, the suggested approach would address the concerns raised by the FDA by requiring such documents to be signed and the required controls to be put in place before the document was used officially.

61. *. .. The* agency *expects that, by their nature, some procedures and controls, such as use of time-stamped audit trails and operational checks, will be built into hardware and software. . . .*

Most current systems will have a range of such controls but they are unlikely to directly match those required by the Regulation. Hence, it will be necessary for companies to upgrade or replace systems to achieve compliance requiring significant time and expense.

69. . . . Proposed I I. IO(b) states that controls for closed systems must include the ability to generate true copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency, and that if there were any questions regarding the ability of the agency to perform such review and copying, persons should contact the agency. . . .

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

71. *. . . Proposed II. IO(c) states that procedures and controls for closed systems must include the protection of records to enable their accurate and ready retention throughout the records retention period . . .*

The rapid obsolescence of technology means that systems have a life cycle on the order of 5-7 years. Hence, it is unlikely that systems that can fully process the data in electronic form will be available over the required retention period of the electronic records. Hence, FDA and the industry will need to work together to agree on durable standards such as Oracle and SAS data sets and PDF document formats that have the potential to be supported over the time frames required.

72. . . . The agency considers such operator actions as activating a manufacturing sequence or turning off an alarm to warrant the same audit trail coverage as operator data entries in order to document a thorough history of events. . . .

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

73. . . . To maintain audit trail integrity, the agency believes that it is vital that the audit trail can be created by the computer system independently of operators, ...

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

85. . Proposed 11.I 0(h) states that procedures and controls for closed systems must include the use of device (e.g. terminal) location checks to determine, as appropriate, the validity of the source of data input or operational instruction. . . .

Most modern client server-based systems do not support this kind of check. Authentication checks focus on who is using the system and what level of access and authorization they have rather than the physical point of access. Hence, it is unclear whether vendors would be willing to support such a requirement. Assuming they will, such an approach will require current systems to be upgraded or replaced and is likely to be time consuming and expensive to implement and support.

IX. Electronic Records - Signature Manifestations (11.50)

98. . ..The printed name of the signer (at the time the record is signed as well as whenever the record is read by humans); (2) the date and time of signing; and (3) the meaning of the signature, . . .

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

101 . . .*.Regarding systems that may span different time zones, the agency advises that the signer 's local time is the one to be recorded. . .*

Given the growing use of more centralized computing systems for business critical processes, this raises a number of issues. Since a central system may be supporting users in multiple time zones, the use of local times requires the user to enter the time of the transaction or to rely on the time sent by the local user device which may not be correct. This compares with using timestamps provided by the central system which will normally have a high degree of accuracy.

The second point is that where actions are carried out on multiple sites in multiple time zones it will now be much more difficult to establish the sequence of events, since the times recorded by the central system are not consistent. From the perspective of the central system, it will also be possible to record future actions if they are received from a time zone ahead of that of the central system.

Because of these problems, most systems that span multiple time zones record time based on a single standard and this is something that the FDA may wish to consider. In accordance with good practice, the industry would recommend the use of a standard time for such systems.

XII. Electronic Signature Components and Controls (11.200)

123. . ..Employ at least two distinct identification mechanisms (such as an identification code andpassword), each of which is contemporaneously executed at each signing...

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

124. . . . *use of automatic inactivity measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe....*

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

XVI. Analysis of Impacts

. . . The Unfunded Mandates Act requires that agencies prepare an assessment of anticipated costs and benefits before proposing any rule that may result in an annual expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million (adjusted annually for inflation). . . .

The cost to the industry of achieving compliance with the Regulation is well in excess of $100 million. The fact that the industry already makes extensive use of electronic systems means that the option of returning to paper based submissions is non-viable,

. ..The activities regulated by this rule are voluntary; no entity is required by this rule to maintain or submit records electronically...

The fact that the industry already relies heavily on the use of electronic systems means that compliance with the Regulation is not voluntary, as it is not viable for companies to return to paper-based systems.

C. Description of Impact

. . . Furthermore, because almost all *of the rule's provisions reflect contemporary security measures and controls that respondents to the ANPRM identified, most firms should have to make few, if any, modifications to their systems. . . .*

Most companies rely heavily on electronic systems. It is highly unlikely that these systems will meet the specific requirements of the new Regulation. Hence, most companies will have to embark on a major upgrade and/or replacement cycle to meet the requirements.

... The agency believes that because the rule is flexible and reflects contemporary standards, firms should have no difficulty in putting in place the needed systems and controls. . . .

It normally takes a significant period of time for new technologies to become incorporated into major software packages, particularly those used in regulated environments. Many of the technologies required to support electronic signatures and authentication, particularly those based on the use of a Public Key Infrastructure, are still at an early stage of development and it is likely to be several years before they are incorporated into major commercial software packages.

Appendix B
Comments on 21 CFR Part 11 Regulation

11.3 Definitions

4. . Closed system means an environment in which system access is controlled by persons who are responsible for the content of the electronic records that are on the system...

The users responsible for the contents of the electronic records in a system are almost never responsible for directly authorizing system access. This is done by a company's IS staff, or their authorized agents. Hence, it is proposed that a system in which users control access, which is physically implemented by the company's IS staff or their agents, be considered closed.

11.10 Controls for Closed Systems

a . . . *the ability to discern invalid or altered records...*

Altered records can be tracked by means of the required audit trail. Invalid records can be detected by a number of tests but an invalid record may still meet the requirements of such tests. Hence, the above statement should be interpreted on the basis of those invalid records that it is reasonable to detect. Requirement of computerized audit trail for "which records and/or at what stage(s) of record?" still needs to be resolved.

b.. *The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency...*

Most current systems will need to be upgraded or replaced to meet this requirement.

c...*Protection of records to enable their* accurate *and ready retrieval throughout the records retention period..*

Given the rapid obsolescence of technology, it will be necessary to agree on a core set of standards, such as Oracle and SAS data sets and PDF document formats, that are likely to endure over the required retention periods.

e... Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retainedfor a period at least as *long as that requiredfor the subject electronic records and shall be available for agency review and copying..*

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance. The issue of time zones arises for many systems. Most such systems employ a common standard time but the guidelines propose the recording of local time which can give rise to a number of problems.

f.. *Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate...*

This is difficult to do if the system spans multiple time zones and records local times. Hence this reinforces the recommendation to use a standard time for such systems.

h... Use *of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction...*

These checks are not supported by most modern systems based on a client server architecture. Authentication checks focus on who is using the system and what level of access and authorization they have, rather than the physical point of access. Even if vendors are willing to support such an approach it is likely to take years and will be expensive to implement and support.

11.30 Controls for Open Systems

. ..Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality...

Document encryption and digital signatures are new technologies that are still at an early stage of development. Document encryption is also complicated by the fact that the US government imposes export restrictions on this technology. Normally, there will be a significant delay before such technologies are incorporated into major commercial software packages. To ensure authentication and non-repudiation, a Public Key Infrastructure is required and this is also at a very early stage of development.

11.50 Signature Manifestations

... (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following.
(I) The printed name of the signer.
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
(b) The items identified in paragraphs (a)(l), (a)(Z), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)...

These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

11.200 Electronic Signature Components and Controls

. ..*subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual...*

Most of the major commercial software packages in use in the industry do not operate in this manner. These are new requirements that will require companies to upgrade or replace current systems to achieve compliance.

11.300 Controls for Identification Codes/Passwords

b.. . *Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)...*

Most major operating systems allow for password aging. They vary considerably in enforcing rules on the length and composition of passwords, the degree of difference required between subsequent passwords and the frequency with which they can be reused. Since the operating system is normally the most secure and trusted software element in a computer system, the industry recommends relying on these whenever possible and augmenting them with standard operating procedures (SOPs).

d... *Use of transaction safeguards to prevent unauthorized use ofpasswords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management...*

Modern system environments are comprised of large numbers of interconnected systems. In these complex environments, security focuses on preventing unauthorized users from gaining access. Most operating systems provide the facility to disable an account after a specified number of failed attempts and similar abilities may be included in some major software packages.

In most cases, a printout of disabled accounts can be obtained to allow follow-up. Most systems do not support the immediate reporting of access failures and, since access is normally disabled after a small number of tries, systematic attempts to discover passwords are normally inhibited.

Since expired and forgotten passwords are one of the most common causes of helpdesk calls, an immediate reporting system would tend to overwhelm company security units and the large proportion of legitimate failures would quickly serve to desensitize the system, Hence, a more appropriate approach may be to require the routine auditing of disabled accounts with selective follow up of suspicious cases.